

## Practical-2A

Steps:-

1. Download ceptool, then Install.
2. Open Ceptool  
→ file → New
3. Now Enter plain text to ~~dec~~-encrypt.
4. Click on Encrypt/Decrypt → Symetric (modeen)  
→ RC4 → Enter key length as 16 bit  
→ click on Encrypt.
5. Text will be converted to ciphertext.
6. Now again click on Encrypt/Decrypt  
→ Symetric (modeen) → RC4 → Enter  
key length as 16 bit → click on  
Decrypt.
7. Now Decrypted text will be visible.

## Peactical-3A

Aim: Run & analyze the output of following commands in Linux - ifconfig, ping, netstat, teaceout.

Steps:

1. Open cmd. & execute following commands:  
To change directoy use : >cd..

① ping : verifies the connectivity to another tcpip computer.

>ping www.google.com

② ipconfig : shows ip address of the system.  
>ipconfig

③ teaceet : Analyze the different paths in your network to find the fastest path following the shortest path protocol.

>teaceet www.google.com

④ netstat : Display network statistics for all active Network connections & ports.

>netstat

## Practical-3b

Aim: ARP poisoning.

Steps:

Step 1. Open cmd with admin access.

change directory.

C:\>Users\Administrator>cd..

C:\>Users>cd..

C:\>

Step 2. Execute following commands:

① ipconfig : Gives detailed information about all the network connections available in your computer.

>ipconfig

② ipconfig / all : Gives the IP & MAC address of your computer.

Step 3 Write down your IP address i.e.

IPv4 Address : 192.168.7.74

and MAC address i.e. Physical Address

70-54-D2-19-8F-7A. Displayed in cmd.

④ arp : Calls the ARP configure program located in windows\system32 directory  
>arp.

⑤ `>arp -s [Device-IP][Device-MAC]`  
arp-s creates a static ARP mapping between IP & MAC address

⑥ `>arp -a` : Display the contents of the ARP cache.

⑦ `>arp -d` : Delete ARP entry for IP address.

`>arp -d [Device-IP]`

⑧ `arp -a` : To check the ARP entry has been removed.



## Practical-4

Aim: Use NMap Scanner to perform port scanning of various ports - ACK, SYN, FIN, FULL, XMAS.

### Steps:

1. download and install Nmap.
2. Open Nmap folder in program files and open with cmd.
3. Now execute following commands.
  - ① nmap
  - ② nmap -sA -T4 scanme.nmap.org
  - ③ nmap -p22,113,139, scanme.nmap.org
  - ④ nmap -sT -T4 puec
  - ⑤ nmap -sN -p22 scanme.nmap.org
  - ⑥ nmap -sX -T4 scanme.nmap.org

## Practical-5A

Aim: Use Wireshark to capture Network traffic.

Steps:

1. Download and Install Wireshark.
2. Open browser and search for test.php.vulnerable web.
  - Open first website.
  - Open login page & enter username and password.
3. Open Wireshark.
  - Type Http in search bar.
  - find out login.php file in the list appeared.
  - Right click on login.php file
  - follow
  - TCP Stream.
4. Username & Password you have entered will be visible.

# LOIC - Low Orbit Ion Cannon Tool

PAGE No.	
DATE	/ /

## Practical - 5B

Aim : Use <sup>LOIC</sup> ~~Nemesy~~ to launch DOS attack

Steps :-

1. ~~Se~~ Open browser search LOIC.exe Github and download zip.
2. Turn off Security Threats in Windows.
3. Extract zip file and open LOIC application.
4. Search for test.php.vulnerable web in browser and copy URL.
5. Paste URL in first textbox. → Lock on.  
→ Enter IP address visible on screen in the second text box.  
→ Choose TCP stream in dropdown.  
→ Click on CHARGING MY LASER button to start DOS attack.
6. Click on stop flooding to stop attack.

## Practical-6

Aim: Simulate persistent cross-site scripting.

Steps:

1. Download & Extract DVWA.
2. Download & Install XAMPP server.
3. Copy extracted DVWA folder and paste in C:\drive\xampp\htdocs directory.
4. Open config file in DVWA folder.  
 → Rename config.php file by removing dist extension.  
 → open config.php change servername as root & keep password empty.
5. Search for CSS payload github and copy script.  
`<script> alert('xss') </script>`
6. Open <sup>& start</sup> XAMPP server  
 → type http://localhost/DVWA/ in browser.
7. Click on DVWA security and set security level as low.




8. Go to XXS (Stored)  
 → click on create/Reset Database.

9. Now type name & script on textbox.  
 → click on Sign Guest Book.

## Practical-7

### A. Session Impersonation.

- Steps:

1. Open browser and search EditThis cookie extension.  
→ Add extension to Chrome.
2. Click on extension icon in Right corner in browser.
3. Click on Export   
→ Open Notepad & paste cookie content.
4. Click on Delete Button to delete Cookie.

### B. Tamper Data Add-on.

Steps.

1. Search Tamper Data add-on Extension.  
→ add extension to firefox.
2. Search Tibetan modonata open to first Link.  
→ Open login page enter Username and password.
3. Click on ~~ex~~ cloud icon in Right corner and you will see the tampered data.

## Practical-8

Aim: SQL injection.

Steps:-

1. Download and Extract DVWA.
2. Download and Install Xampp Server.
3. Copy extracted DVWA file and locate in C drive / xampp / htdocs directory.
4. Open config file in DVWA folder.
  - remove dist extension.
  - Open file with notepad and
  - change database user as root.
  - remove password in Database configuration.
5. Open & start Xampp Server.
  - type localhost / DVWA in browser.
6. Go to DVWA security
  - select low and submit.
7. Go to SQL inject.
  - create / Reset Database.

8. Enter search for SQL payload Github in browser.  
→ copy payload script.
9. Enter copied script in Use Id Textbox & all users data from database will be fetched.



## Practical-9

Aim : Keylogger using Python.

Steps :

1. Create a folder in file explorer.
2. Open that folder with VS code or any other code editor.
3. Create a new file with .py extension.
4. Write down python code for keylogger  
→ Run the file.
5. You will get a Security Thread Prompt.  
→ Allow Threat in windows security.
6. Python file gets deleted, you have to save it again with the same name.
7. Now a text file will get created which contain keyboard inputs.